

REMARKS

Claims 1-12 and 14-26 are pending in the application. Applicant reserves the right to pursue the original claims and other claims in this and other applications.

Claims 1, 8, 15, 17, and 20 have been amended. No new matter has been added.

Claims 1, 6-8, 14-20 and 26 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Serecki et al (U.S. Pat. Pub. No. 20030078072)("Serecki"). This rejection is respectfully traversed.

Claim 1 recites, *inter alia*, a method of updating an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising "physically separating from said wireless station a network communication device containing said encryption key which is accessed for use by said wireless station during said encrypted communications; physically connecting said removed network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; and physically reconnecting said network communications device containing said new encryption key with said wireless station of said network."

Serecki discloses "A method for providing configuration information for use in installing a new wireless station to a wireless network that minimizes errors is presented. The configuration information is distributed by storing the configuration information onto a device with a memory and then distributing the device to the users interested in installing new wireless stations. The device is attached to a computer to

which the wireless station is coupled, initiating a transfer of the configuration information. The computer uses the configuration information to configure the wireless station. The method also provides a way to limit access to the configuration information through the use of encryption and limiting the number of times the configuration information is retrieved. The method is also an effective way to distribute security keys for encryption systems whose purpose is to secure communications in a wireless network. " (Serecki, Abstract)

Serecki fails to disclose "physically separating from said wireless station a network communication device containing said encryption key which is accessed for use by said wireless station during said encrypted communications." To the contrary, the invention of Serecki is essentially a method of transferring information between two computers systems that are not physically connected by using a storage device as a conduit between the two systems, e.g., a "wireless station" and a "wired portion of a network". Thus in the invention of Serecki, a storage device is used to transfer data, e.g., configuration information or security keys, between the two systems. As such, the invention of Serecki is different from the claimed invention and the rejection of this claim should be withdrawn for at least the reason noted.

Claims 6-7 depend from claim 1 and are allowable for at least the reason noted above with respect to claim 1.

Claims 8, 14-20 and 26 have similar limitations as claim 1 and are allowable for at least the reason noted above with respect to claim 1.

Claims 2-3, 9-10, and 21-23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serecki. This rejection is respectfully traversed.

Claims 2-3, 9-10, and 21-23 have similar limitations as claim 1 and are allowable for at least the reason noted above with respect to claim 1.

Additionally, the Examiner indicates that "Serecki does not explicitly disclose a method wherein a new encryption key is a randomly generated encryption key. However, it would have been obvious to a person having ordinary skill in the art...to modify the method disclosed by Serecki..." However, the Examiner provides no support for this position. Rejections must be based on objective facts and teachings of references.

A statement that modifications of the prior art to meet the claimed invention would have been "well within the ordinary skill of the art at the time the claimed invention was made" because the references relied upon teach that all aspects of the claimed invention were individually known in the art is not sufficient to establish a *prima facie* case of obviousness without some objective reason to combine the teachings of the references. *Ex parte Levengood*, 28 USPQ2d 1300 (Bd. Pat. App. & Inter. 1993). See also *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1318 (Fed. Cir. 2000) (Court reversed obviousness rejection involving technologically simple concept because there was no finding as to the principle or specific understanding within the knowledge of a skilled artisan that would have motivated the skilled artisan to make the claimed invention); *Al-Site Corp. v. VSI Int'l Inc.*, 174 F.3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999) (The level of skill in the art cannot be relied upon to provide the suggestion to combine references.). MPEP 2143.01

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165

USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). MPEP 2143.03

The Examiner has provided no references to support the argument that it would have been obvious. As such, the rejection of claims 2-3, 9-10, and 21-23 should be withdrawn.

Claims 4-5, 11-12, and 24-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Serecki in view of Triefer et al (U.S. Pat. No. 6,226,750). This rejection is respectfully traversed.

Triefer discloses "A method and system for tracking communications in a client-server environment. The method includes the steps of sending a first request from the client to the server over a first connection, sending a first key from the server to the client over the first connection, sending the first key from the client and a second request to the server over a second connection, and sending a response to the second request and a second key distinct from the first key from the server to the client over the second connection. The system includes a client for establishing a terminal connection with a server and a server in communication with the client. The server further includes key generator means generating a plurality of keys for transmission to the client, authentication means in communication with the key generator means receiving the keys from the client to recognize the keys at the server, and discarding means linked to the key generator means for disposing of previously transmitted keys." (Triefer, Abstract)

With respect to claim 1, Triefer fails to disclose "a network communication device containing said encryption key which is accessed for use by said wireless station

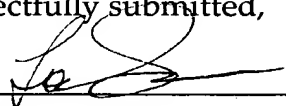
during said encrypted communications.” As such, Trieger does not supply the deficiency of Serecki. At most, Trieger discloses a server that can generate a key. As such, Trieger’s invention is different from the invention of claim 1.

Claims 4-5, 11-12, and 24-25 have similar limitations as claim 1 and are allowable for at least the reason noted above with respect to claim 1.

In view of the above amendment, applicant believes the pending application is in condition for allowance.

Dated: September 7, 2006

Respectfully submitted,

By 

Thomas J. D'Amico

Registration No.: 28,371

Michael A. Weinstein

Registration No.: 53,754

DICKSTEIN SHAPIRO MORIN &

OSHINSKY LLP

2101 L Street NW

Washington, DC 20037-1526

(202) 785-9700

Attorneys for Applicant